



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,352	11/13/2001	Art Shelest	212159	8322

23460 7590 03/07/2005

LEYDIG VOIT & MAYER, LTD  
TWO PRUDENTIAL PLAZA, SUITE 4900  
180 NORTH STETSON AVENUE  
CHICAGO, IL 60601-6780

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/010,352

Applicant(s)

SHELEST ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 November 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-17, 21 and 22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-17, 21 and 22 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

***DETAILED ACTION***

1. This action is in response to request for reconsideration filed on November 29, 2004. Claims 18 – 20 were cancelled. No new Claims were added. Therefore, presently pending claims are 1 – 17, 21 and 22.

***Terminal Disclaimer***

2. The terminal disclaimer filed on November 29, 2004 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 09/833,922 has been reviewed and is accepted. The terminal disclaimer has been recorded.

***Response to Arguments***

3. Applicant's arguments filed on November 29, 2004, have been fully considered but they are not persuasive for the following reasons:

4. Applicant argued that the cited prior art (CPA) [Diffie (U.S. Patent number RE.36,946, hereafter "Diffie")] does not teach, suggest or disclose "the network address having a portion derived from the public key of the first computing device", "the message including the digital signature in a packet option", "deriving a portion of a

second network address from the public key of the first computing device" and "accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address".

5. Diffie teaches a method for providing a secure communication between two devices by sending a digital signature, which contains a binding between the public key and machine name (network address) that is digitally signed using a private key and both parties exchange certificates for future data transfer (Column 1 line 49 – Column 2 line 20; Column 7 lines 6 – 10 and Column 10 lines 14 – 35). Both devices verify all messages (digital signature with public key information of the both device) and authenticate before processing or before entering data transfer phase (Column 8 lines 7 – 64 and Column 10 lines 41 – 45).

6. Regarding Claims 1 and 2, Diffie teaches and describes a method for a first computing device to make authentication information (message) including public key of the first computing device, a digital signature, a binding between the public key and a logical identifier of the machine (network address) having a portion derived from the public key of the first computing device (Column 1 line 49 – Column 2 line 20 and Column 8 lines 7 – 23 and 41 – 48).

Diffie further teaches that the message will include public key of the first and second device along with logical identifier of the machine (network address) wherein the

certificate is digitally signed by the private key of the first device (Column 8 lines 49 – 67).

7. Regarding Claim 3, 6, 8-11, 17 and 21, Diffie teaches and describes a method for a first computing device to make authentication information (message) including public key of the first computing device, a digital signature, a binding between the public key and a logical identifier of the machine (network address) deriving a portion of a second network address from the public key of the first computing device (Column 1 line 49 – Column 2 line 20 and Column 8 lines 7 – 23 and 41 – 48).

Diffie also teaches accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address (Column 8 7 – 23 and 41 – 67) where the first device verifies the authentication information and if the certification is valid then verifies the public key of the second device (network address which is a binding between the public key and the machine name of the second device).

8. Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent claims 1-3, 5, 6, 8-11, 17 and 21. Dependent claims 4, 7, 12-16 and 22 are also rejected at least by virtue of their dependency on independent claims and by

other reason set forth in this and previous (October 01, 2004) office action. Accordingly, the rejection for the pending Claims 1 – 17, 21 and 22 is respectfully maintained.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1 – 17, 21 and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Diffie et al (U.S. Patent Number Re. 36,946).

10. Regarding Claims 1 and 2, Diffie teaches and describes a method for a first computing device to make authentication information available to a second computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

creating authentication information, the authentication information including content data, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a private key of the first computing device corresponding to the public key,

the digital signature generated from data in the set: the content data, a hash value of data including the content data (Fig. 4a – 4c, 5a; and Column 1 line 49 – Column 2 line 20 and Column 7 lines 6 – 45); ; and

making the authentication information available to the second computing device, in part by sending a message to the second computing device, the message including the second digital signature in a packet option (Column 6 line 60 – Column 7 line 10 and Column 9 line 46 – Column 10 line 9).

11. Regarding Claims 3 and 5, Diffie teaches and describes a method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58);

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data a hash

value of data including the content data, wherein the second computing device accesses the public key of the first computing device over an insecure channel, and wherein if the content data are not accepted, then the public key is discarded (Column 7 line 46 – Column 8 line 58 and Column 12 lines 13 – 36).

**12.** Regarding Claims 6 and 8, Diffie teaches and describes a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

hashing the public key; comparing a porting of a value produced by the hashing with a portion of the network address other than the non-selectable portion; if the portions do not match, choosing a modifier, appending the modifier to the public key, and repeating the hashing and comparing, and if the portions match, setting the node-selectable portion of the network address to a portion of the value produced by the hashing (Column 5 line 59 – Column 6 line 7; Column 7 lines 6 – Column 8 lines 67; Column 10 lines 41 – 47; and Column 11 lines 58 – 67).

**13.** Regarding Claim 9 and 10, Diffie teaches and describes a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device and from a route prefix of the network address of the computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:



hashing the public key and at least a portion of the route prefix of the network address; setting the node-selectable portion of the network address to a portion of the value produced by hashing; checking to see if the network address as set is already in use; and if the network address as set is already in use, choosing a modifier, appending the modifier to the public key, and repeating the hashing, setting, and checking (Column 5 line 59 – Column 6 line 7; Column 7 lines 6 – Column 8 lines 67; Column 10 lines 41 – 47; and Column 11 lines 58 – 67).

**14.** Regarding Claims 11 and 17, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature; deriving a portion of a second network address from the public key of the first computing device; validating the digital signature by using the public key of the first computing device (Fig. 4a – 4c, 5a, 5b; and Column 1 line 49 – Column 2 line 20 and Column 7 line 46 – Column 8 line 58); and

caching the public key in association with the first network address if the derived portion of the second network address matches a corresponding portion of the first

network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data (Column 7 line 38 – Column 10 line 53; Column 11 line 58 - 67 and Column 12 line 13 – 30).

**15.** Regarding Claim 21, Diffie teaches and describes a computer-readable medium having stored thereon a data structure of authentication information, the data structure comprising:

a first data field containing data representing a public key of a computing device; and a second data field containing data representing a network address of the computing device, the network address derived, at least in part, from a hash of the public key (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53).

**16.** Claim 4 is rejected as applied about in rejecting Claim 3. Furthermore, Diffie teaches and describes a method for a second computing device to authenticate content data made available by a first computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the second computing device accesses the public key of the first computing device over an insecure channel to a device in the set: the first computing device, a key publishing device (Column 7 38 – 55).

17. Claim 7 is rejected as applied about in rejecting Claim 6. Furthermore, Diffie teaches and describes a method for a computing device to derive a node-selectable portion of a network address from a public key of the computing device (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the portion of the address other than the node-selectable portion comprises an element in the set: “u” bit, “g” bit, a portion of a route prefix (Column 5 line 59 – Column 6 line 25).

18. Claim 12 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address (Column 7 line 41 – Column 8 line 11).

19. Claim 13 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

determining whether to cache the public key in association with the first network address based on a time stamp in the authentication information (Column 3 lines 45 – 52).

Art Unit: 2136

**20.** Claim 14 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

comparing the first network address against a network address in a public key/network address in a public key/network address association already in the cache; and if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then discarding the public key and the first network address without caching them (Column 7 line 38 – Column 10 line 47).

**21.** Claim 16 is rejected as applied about in rejecting Claim 11. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

associating a timer with the caching of the public key/network address association; resetting the timer if a second public key/network address association, identical to the public key/network address association, is presented for caching; and if the timer expires, removing the public key/network address association from the cache (Column 7 line 38 – Column 10 line 47).

**22.** Claim 22 is rejected as applied about in rejecting Claim 21. Furthermore, Diffie teaches and describes a computer-readable medium having stored thereon a data structure, (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

a third data field containing data representing a time stamp (Column 7 line 7 – 10).

**23.** Claim 15 is rejected as applied about in rejecting Claim 14. Furthermore, Diffie teaches and describes a method for a second computing device to maintain a cache of at least one public key/network address association (Fig. 2, 3, 4a – 4c, 5a, 5b; and Column 4 line 6 – Column 10 line 53), further comprising:

if the first network address matches the network address in the public key/network address association already in the cache, and if the public key does not match a public key of the public key/network address association already in the cache, then removing from the cache the public key/network address association already in the cache (Column 10 lines 41 – 52).

### ***Conclusion***

**24.** The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

**25. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.


Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy

February 26, 2005.



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100